

TOR ANONYMITY HOWTO

by Cyber Anarchy

Τι είναι το Tor?

Το Tor είναι ένα πρόγραμμα που (είτε μας αρέσει είτε όχι) αναπτύχθηκε αρχικά από το Αμερικανικό Ναυτικό για να προσφέρει ανωνυμία στο διαδίκτυο. Στη συνέχεια έγινε ανοιχτού κώδικα και από τότε αναπτύσσεται από την κοινότητα του και από διάφορους οργανισμούς.

Πως λειτουργεί?

Πολύ απλά και συνοπτικά η λειτουργία του Tor είναι η εξής. Υπάρχει ένα δίκτυο, το λεγόμενο Tor network, που αποτελείται από διάφορους server (nodes). Το πρόγραμμα συνδέεται στο δίκτυο αυτό και μεταφέρει τα πακέτα από node σε node, μέχρι αυτά να φτάσουν στην άλλη άκρη (π.χ την ιστοσελίδα που θέλουμε).

Τι δεν είναι το Tor

Το Tor δεν προσφέρει σε καμία περίπτωση 100% ανωνυμία. Όπως άλλωστε γράφει και το πρόγραμμα :

```
[notice] Tor v0.1.2.17. This is experimental software. Do not rely on it for strong anonymity.
```

Τι σημαίνει αυτό? Ότι πολύ απλά, ο εντοπισμός δεν είναι αδύνατος. Το Tor από μόνο του μπορεί να προσφέρει ανωνυμία στο επίπεδο που δεν είναι καθόλου εύκολο για τον καθένα να δει από που γίνεται πραγματικά η σύνδεση. Όμως υπάρχουν τεχνικές με τις οποίες κάποιος παρακολουθώντας την κίνηση του δικτύου Tor να βρει την αρχική πηγή. Από εκεί και πέρα υπάρχουν τρόποι με τους οποίους η δουλειά αυτή μπορεί να γίνει ακόμη δυσκολότερη, αλλά ποτέ αδύνατη.

Εγκατάσταση Tor client (Linux)

Το Tor είναι αρκετά διαδεδομένη εφαρμογή, επομένως υπάρχουν έτοιμα πακέτα για πολλές διανομές. Το guide που ακολουθεί (σε όσα σημεία χρειαστεί) έχει γραφτεί αρχικά για Ubuntu (στο 90% του guide το λειτουργικό δεν παίζει ρόλο).

Ας ξεκινήσουμε με την εγκατάσταση.

1. Ανοίγουμε το Synaptic
2. Settings--->Repositories--->Third-Party Software--->Add

και βάζουμε την εξής γραμμή :

```
deb http://mirror.noreply.org/pub/tor <DISTRIBUTION> main
```

οπου <DISTRIBUTION> η διανομή που χρησιμοποιούμε(π.χ gutsy)

3. Ανοίγουμε ένα terminal και πληκτρολογούμε

```
sudo apt-get install tor
```

4. Κάνουμε ένα restart και το Tor client είναι έτοιμο!

Αυτή την στιγμή έχουμε το Tor client εγκατεστημένο στο σύστημα μας, όμως δεν έχουμε δρομολογήσει καμία σύνδεση να περνάει από αυτό. Ας ξεκινήσουμε με την βασικότερη λοιπόν που είναι φυσικά ο web browser.

Εγκατάσταση του Privoxy

Για να γίνει αυτό θα χρειαστεί να εγκαταστήσουμε άλλο ένα πακέτο, το οποίο υπάρχει ήδη στα repositories μας, το privoxy. Ανοίγουμε λοιπόν άλλη μια φορά το terminal και γράφουμε

```
sudo apt-get install privoxy
```

Εδώ θα πρέπει να γίνουν μερικές ρυθμίσεις. Πηγαίνουμε λοιπόν στο αρχείο config του Privoxy που βρίσκεται στο /etc/privoxy/ (αυτό πρέπει να γίνει με δικαιώματα root).

Προσθέτουμε την παρακάτω γραμμή στην αρχή του αρχείου. Μην ξεχάσετε την τελεία στο τέλος

```
forward-socks4a / 127.0.0.1:9050 .
```

Το Privoxy κρατάει αρχείο από τις συνδέσεις που περνάνε μέσα από αυτό, πράγμα το οποίο δεν θέλουμε στην προκειμένη περίπτωση. Για να το απενεργοποιήσουμε ψάχνουμε τις επόμενες γραμμές και βάζουμε ένα # στην αρχή της κάθε γραμμής.

```
logfile logfile  
jarfile jarfile
```

(και σε μερικά συστήματα την γραμμή)

```
debug 1 # show each GET/POST/CONNECT request
```

Στη συνέχεια το μόνο που μένει να κάνουμε είναι να εγκαταστήσουμε στον Firefox το extension Torbutton, το οποίο θα το βάλουμε στην ρύθμιση Use Privoxy.

Χρήση του Tor σε άλλες εφαρμογές

Οι εφαρμογές που μπορούν να χρησιμοποιήσουν Tor είναι πάρα πολλές. Ο γενικός “κανόνας” με τον οποίο μπορούν να ρυθμιστούν οι περισσότερες είναι ο εξής.

1. Ψάχνουμε μέσα στο πρόγραμμα για την επιλογή χρήσης proxy.
2. Σαν proxy ορίζουμε το localhost και port την 9050. Αν υπάρχει και επιλογή πρωτοκόλλου βάζουμε SOCKS (ή SOCKS4).

Tor Server

Γιατι να γίνει κάποιος Tor Server ?

Για 2 κύριους λόγους :

1. Διότι προσφέροντας bandwidth βελτιώνει την ποιότητα του δικτύου Tor.
2. Διότι προσφέρει στον εαυτό του μεγαλύτερη ανωνυμία αφού δεν μπορεί κάποιος να ξέρει αν η σύνδεση έγινε πραγματικά απο τον υπολογιστή του ή από κάποιον που είχε συνδεθεί στον server που έτρεχε ο υπολογιστής αυτός.

Ρυθμίσεις Tor Server

Για να γίνει κάποιος Tor Server δεν χρειάζεται κάποιο άλλο πρόγραμμα. Μόνο κάποιες μικρές αλλαγές στο configuration file του Tor.

Ανοίγουμε λοιπόν ξανά το αρχείο torrc. Πάμε στο κάτω μέρος του αρχείου που αφορά τον server. Ουσιαστικά οι μόνες απαραίτητες ρυθμίσεις είναι το Nickname και το ORPort (αυτές οι 2 γραμμές θα πρέπει να γίνουν uncomment, δηλαδή να φύγει το # που υπάρχει μπροστά).

Βεβαιωθείτε (αν έχετε firewall ή router) να ανοίξετε την ORPort ώστε να μπορεί ο server σας να συνδεθεί με τους υπόλοιπους του Tor network.

Τέλος μετά από οποιαδήποτε ρύθμιση ή αλλαγή στο torrc ή στο config του privoxy απαιτείται ένα restart και στα 2. Αυτό γίνεται δίνοντας την εντολή

```
sudo /etc/init.d/privoxy restart  
sudo /etc/init.d/tor restart
```

Tor Tutorial for Windows

Εισαγωγή – Download του Vidalia Bundle:

Για τα Windows υπάρχει ένα “πακέτο” με 3 εφαρμογές: (Tor, Privoxy, Vidalia) το οποίο λέγεται Vidalia Bundle και κάνει τη ζωή μας εύκολη. Μπορούμε να το κατεβάσουμε από εδώ:

<http://www.torproject.org/download.html.en>

Τρέχουμε το αρχείο που κατεβάσαμε, αφού βεβαιωθούμε ότι έχουμε απεγκαταστήσει τυχόν προηγούμενες εγκαταστάσεις του Tor, του Vidalia ή του Privoxy. Διαλέγουμε Full Install και περιμένουμε να τελειώσει η εγκατάσταση.

Για την ρύθμιση του Tor το πρώτο βήμα είναι η ρύθμιση του Web Browser.

Ρύθμιση για Mozilla Firefox (προτείνεται):

Αν έχετε Firefox (ο οποίος γενικά προτείνεται) χρειάζεστε ένα plugin/add-on όπως το Torbutton. (Υπάρχει στο πακέτο, αλλά μπορείτε πολύ εύκολα να το εγκαταστήσετε και από την διεύθυνση: <https://addons.mozilla.org/firefox/2275/>). Μετά την εγκατάστασή του χρειάζεται επανεκκίνηση ο Firefox. Θα εμφανιστεί κάτω στην μπάρα του Firefox το κουμπί εναλλαγής Tor Disabled/Tor Enabled, με το οποίο μπορείτε να ενεργοποιείτε ή να απενεργοποιείτε το Tor.

Ρύθμιση σε διαφορετικό browser και σε άλλες εφαρμογές:

Για την ρύθμιση διαφορετικού Web Browser, θα πρέπει να κάνετε μόνοι σας τις ρυθμίσεις, βάζοντας την port του Privoxy (8118) και το host: localhost στις ρυθμίσεις για Proxy. Για χρήση SOCKS, η port (default) είναι η 9050. (SOCKS v5)

Για την χρήση σε προγράμματα κατευθείαν με SOCKS, θα πρέπει να χρησιμοποιηθεί η port 9050. Για παράδειγμα σε εφαρμογές Instant Messengers, Telnet, SSH κτλ. μπορείτε κατευθείαν να δηλώσετε host: localhost και port: 9050 και SOCKS v5.

Γενικά το Privoxy εξυπηρετεί τα παρακάτω πρωτόκολλα:

HTTP, FTP, Gopher, SSL. Άρα σε αυτά βάζουμε την port του Privoxy: 8118. Στα υπόλοιπα, όπως αναφέρθηκε, με άμεση σύνδεση σε SOCKS v5 στην port: 9050.

Μετά την ρύθμιση αυτή μπορούμε να δοκιμάσουμε εαν δουλεύει:

Αφού βεβαιωθούμε ότι το Vidalia και το Privoxy τρέχει από τα εικονίδια (μπλε “P” το Privoxy και ένα πράσινο “κρεμμύδι” το Vidalia), ανοίγουμε τον browser μας και πηγαίνουμε στην διεύθυνση <http://torcheck.xenobite.eu/> αφού έχουμε ενεργοποιημένο το Torbutton για τον Firefox και τις σωστές ρυθμίσεις για άλλον browser. Το site αυτό ανιχνεύει εαν είμαστε συνδεδεμένοι στο δίκτυο του Tor και έχουμε “αλλάξει” IP. Εαν δεν συμβαίνει αυτό, ελέγξτε τις ρυθμίσεις του browser σας ή βεβαιωθείτε ότι το Torbutton στον Firefox είναι πατημένο. Επίσης θα πρέπει το εικονίδιο του Vidalia να είναι

“πράσινο” που σημαίνει ότι είναι ενεργό το Tor. Κάνοντας διπλό κλικ στο εικονίδιο του Vidalia μπορούμε να σταματήσουμε το Tor και να αλλάξουμε τις ρυθμίσεις του προγράμματος. Προτείνεται να ξεκινάει το Tor μαζί με το Vidalia και καλό θα ήταν κατά την εκίνηση του H/Y. Επίσης το Control Port του Vidalia να είναι στην port: 9051.

Εαν χρησιμοποιείτε firewall, θα πρέπει να κάνετε το κατάλληλο forwarding για τις ports: 8118 και 9050. Βεβαιωθείτε ότι επιτρέπει connections από τις εφαρμογές σας στις τοπικές ports 8118 και 9050.

Για να δούμε ποιά IP Address χρησιμοποιούμε, πηγαίνουμε σε ένα site που μας δείχνει την IP μας όπως το <http://www.cmyip.com>

Μπορούμε επίσης να αλλάξουμε IP/Identity, πατώντας στην κατηγορία Use New Identity στο κεντρικό panel του Vidalia ή πατώντας δεξί κλικ στο εικονίδιο του Vidalia στο taskbar και μετά New Identity.

Ρύθμιση για Tor Server/Relay:

Για περισσότερη ανωνυμία και ενίσχυση με bandwidth στο δίκτυο του Tor, μπορείτε εύκολα να στήσετε Tor Server.

Κάνοντας διπλό κλικ στο εικονίδιο του Vidalia στο taskbar, εμφανίζεται το Control Panel. Απο εκεί αν επιλέξουμε Setup Relaying θα ρυθμίσουμε τον Tor Server μας. Στο παράθυρο που εμφανίζεται βάζουμε το όνομα του Server μας στην φόρμα: Nickname. Στο Contact Info: το e-mail μας (προαιρετικό αν και καλό είναι να υπάρχει). Στο Server Port είναι η port απ' όπου θα συνδέονται στον Server μας clients και άλλους Tor Servers. Προτείνεται η 9001 και θα πρέπει να είναι ανοικτή στο Firewall μας. Αν έχετε Router, θα πρέπει να γίνει forwarding στις NAT ρυθμίσεις.

Εαν θέλετε να γίνει Mirror το directory με τους Servers του Tor από τον Server σας επιλέξτε την επιλογή Mirror the Server Directory. Η port που θα χρησιμοποιείται πρέπει να είναι διαφορετική με την Server Port και θα πρέπει επίσης να γίνει forward στο Router. Προτείνεται η 9030. Αυτές ήταν οι βασικές ρυθμίσεις.

Στο Bandwidth Limits ορίζετε το upload speed της σύνδεσής σας. Στο Exit Policies, δηλώνεται τις δυνατότητες που θα έχουν οι clients που θα συνδέονται στον Server σας. (Websites, IM, IRC, κτλ). Εάν θεωρείτε ότι πρέπει κάποια από αυτά να μην τα χρησιμοποιούν, τότε μπορείτε να μην τα επιλέξετε.

Μετά την ολοκλήρωση των ρυθμίσεων, θα πρέπει να δείτε τα Messages/Logs (από την κατηγορία Message Log στο κεντρικό panel του Vidalia) ώστε εαν υπάρχει error να το διαπιστώσετε. Εαν όλα είναι εντάξει και οι ports είναι ανοικτές και οι ρυθμίσεις του firewall επιτρέπουν connections, τότε δεν θα δείξει κανένα error.

Μπορείτε να δείτε στατιστικά του bandwidth στην κατηγορία: Bandwidth Graph του κεντρικού Control Panel του Vidalia. Δηλαδή τα δεδομένα που στέλλονται και λαμβάνονται στον Server σας με την βοήθεια γραφήματος.

Στην κατηγορία View Network φαίνεται ο χάρτης του δικτύου του Tor και η λίστα με τους διαθέσιμους Tor Servers. Θα πρέπει να εμφανιστεί και ο δικός σας server μαζί με τα στατιστικά σύνδεσης.